

What is claimed is:

- 1 1. A method for initializing a series of electronic
2 transactions, comprising the steps of:
3 a. receiving an initialization request message that
4 atomically binds
5 i. authorization data, and
6 ii. a blinded unvalidated certificate to be
7 validated;
8 b. determining if the authorization data is valid;
9 c. if the authorization data is valid, then
10 validating the blinded unvalidated certificate
11 to obtain a blinded validated certificate; and
12 d. sending an initialization response message to a
13 registrant that includes the blinded validated
14 certificate atomically bound to the
15 initialization request message received in step
16 a.
- 1 2. The method of claim 1, further comprising the step of
2 receiving a registration acknowledgment message from a
3 registrant acknowledging that the registrant has received
4 the initialization response message.
- 1 3. The method of claim 1, wherein the initialization
2 request message includes a nonce, a session key and a
3 blinding factor applied to the nonce, and further
4 comprising the step of storing the initialization request
5 message and the initialization response message in a
6 recovery database.

- Sub
a3
4. A method for recovering from an interruption in
initializing an electronic transaction, comprising the
steps of:
- a. receiving a first initialization request message
from a registrant that includes a nonce, a session key,
and a blinding factor applied to the nonce, and that
atomically binds
 - i. authorization data, and
 - ii. a blinded unvalidated certificate to be
validated;
 - b. storing the initialization request message in a
recovery database;
 - c. determining if the authorization data is valid;
 - d. if the authorization data is valid, then
validating the blinded unvalidated certificate
to obtain a blinded validated certificate;
 - e. sending a first initialization response message
to a registrant that includes the blinded
validated certificate atomically bound to the
initialization request message received in step
a;
 - f. storing the first initialization response
message in a recovery database;
 - g. receiving a second initialization request
message;
 - h. determining if the second initialization request
message has the same nonce, session key, and
blinding factor applied to the nonce as the

29

30

31

32

33

34

35

36

37

38

39

1 5. A method for performing an electronic transaction,
2 comprising the steps of:

3 a. receiving a transaction request message that
4 atomically binds

5 i. an unblinded certificate, and

6 ii. a blinded unvalidated certificate to be
7 validated;

8 b. determining if the unblinded certificate is
9 valid; and

10 c. if the unblinded certificate is valid, then
11 performing a transaction response that includes:

12 i. validating the blinded unvalidated
13 certificate to obtain a validated
14 blinded certificate, and

15 ii. sending the validated blinded
16 certificate atomically bound to the
17 transaction request message to a

18
19
transaction response recipient in a
transaction response message.

1 6. The method of claim 5, wherein the transaction
2 response further includes making available a product to a
3 party.

1 7. The method of claim 5, wherein the transaction
2 response further includes obtaining payment for a product.

1 8. The method of claim 5, further comprising the step of
2 receiving a transaction acknowledgment message from a
3 registrant acknowledging that the transaction response
4 recipient has received the transaction response message.

1 9. The method of claim 5, further comprising the step of
2 storing the transaction request message and the
3 transaction response message in a recovery database.

1 10. A method for recovering from an interruption in an
2 electronic transaction, comprising the steps of:

3 a. receiving a first transaction request message
4 that includes a session key, a nonce and a
5 blinding factor applied to the nonce, and that
6 atomically binds

7 i. an unblinded certificate, and

8 ii. a blinded unvalidated certificate to be
9 validated;

10 b. storing the first transaction request message in
11 a recovery database;

- Sub
a3
- 12 c. determining if the unblinded certificate is
13 valid; and
14 d. if the unblinded certificate is valid, then
15 performing a transaction response that includes
16 i. validating the blinded unvalidated
17 certificate to obtain a validated
18 blinded certificate,
19 ii. sending the validated blinded
20 certificate atomically bound to the
21 transaction request message to a
22 transaction response recipient in a
23 first transaction response message,
24 and
25 iii. storing the first transaction response
26 message in a recovery database;
27 e. receiving a second transaction request message
28 that includes a session key, a nonce and a
29 blinding factor applied to the nonce, and that
30 atomically binds
31 i. an unblinded certificate, and
32 ii. a blinded unvalidated certificate to be
33 validated;
34 f. determining if the second transaction request
35 message has the same nonce, session key, and
36 blinding factor applied to the nonce as the
37 first transaction request message stored in the
38 recovery database; and
39 g. if the second transaction request message has
40 the same nonce, session key, and blinding factor

00635778-084400

41

42

43

44

45

46

47

applied to the nonce as the first transaction request message, then-

- i. retrieving the first transaction response message from the recovery database, and
- ii. sending the first transaction response message to the transaction response recipient.

1 11. A method for auditing an electronic transaction,
2 comprising the steps of:

- 3 a. receiving a transaction request message that
4 atomically binds
 - 5 i. an unblinded certificate,
 - 6 ii. a blinded unvalidated certificate to be
7 validated, and
 - 8 iii. blinded audit data;
- 9 b. sending an audit request message atomically
10 bound to the transaction request message to an
11 audit recipient;
- 12 c. receiving an audit response message atomically
13 bound to the audit transaction message, wherein
14 the audit response message includes audit
15 response data;
- 16 d. determining if the blinded audit data is valid
17 using the audit response data.

1 12. The method of claim 11, wherein the audit response
2 data is determined to be valid if

- 3
4
5
6
- i. the audit response data corresponds to the blinded audit data received in the transaction request message, and
 - ii. the audit response data is legitimate.

1 13. An apparatus for initializing a series of electronic
2 transactions, comprising:
3 a. a processor; and
4 b. a memory that stores instructions adapted to be
5 executed by said processor to,
6 i. receive an initialization request message
7 that atomically binds authorization data
8 and a blinded unvalidated certificate to be
9 validated;
10 ii. determine if the authorization data is
11 valid;
12 iii. if the authorization data is valid, then to
13 validate the blinded unvalidated
14 certificate to obtain a blinded validated
15 certificate; and
16 iv. send an initialization response message to
17 a registrant that includes the blinded
18 validated certificate atomically bound to
19 the initialization request message,
20 said memory coupled to said processor.

1 14. The apparatus of claim 13, further comprising a port
2 adapted to be coupled to a network, said port coupled to
3 said memory and said processor.

Sub
03

1 15. An apparatus for performing an electronic
2 transaction, comprising:
3 a. a processor; and
4 b. a memory that stores instructions adapted to be
5 executed by a processor to
6 i. receive a transaction request message that
7 atomically binds an unblinded certificate
8 and a blinded unvalidated certificate to be
9 validated;
10 ii. determine if the unblinded certificate is
11 valid; and
12 iii. if the unblinded certificate is valid, then
13 to perform a transaction response that
14 validates the blinded unvalidated
15 certificate to obtain a validated blinded
16 certificate, and sends the validated
17 blinded certificate atomically bound to the
18 transaction request message to a
19 transaction response recipient in a
20 transaction response message,
21 said memory coupled to said processor.

1 16. The apparatus of claim 15, further comprising a port
2 adapted to be coupled to a network, said port coupled to
3 said memory and said processor.

1 17. An apparatus for auditing an electronic transaction,
2 comprising:
3 a. a processor; and

- 5 b. a memory that stores instructions adapted to be
6 executed by said processor to
7 i. receive a transaction request message that
8 atomically binds an unblinded certificate
9 and a blinded unvalidated certificate to be
10 validated and blinded audit data;
11 ii. send an audit request message atomically
12 bound to the transaction request message to
13 an audit recipient;
14 iii. receive an audit response message
15 atomically bound to the audit transaction
16 message, where the audit response message
17 includes audit response data; and
18 iv. determine if the blinded audit data is
19 valid using the audit response data,
said memory coupled to said processor.

1 18. The apparatus of claim 17, further comprising a port
2 adapted to be coupled to a network, said port coupled to
3 said processor and said memory.

1 19. An apparatus for recovering from an interruption in
2 an electronic transaction, comprising:

- 3 a. a processor; and
4 b. a memory that stores instructions adapted to be
5 executed by said processor to
6 i. receive a first transaction request message
7 that includes a session key, a nonce and a
8 blinding factor applied to the nonce, and
9 that atomically binds an unblinded

- 11 certificate and a blinded unvalidated
12 certificate to be validated;
13 ii. store the first transaction request message
14 in a recovery database;
15 iii. determine if the unblinded certificate is
16 valid;
17 iv.. if the unblinded certificate is valid, then
18 performing a transaction response that
19 validates the blinded unvalidated
20 certificate to obtain a validated blinded
21 certificate atomically bound to the
22 transaction request message to a
23 transaction response recipient in a first
24 transaction response message, and stores
25 the first transaction response message in
26 a recovery database;
27 v. receive a second transaction request
28 message that includes a session key, a
29 nonce and a blinding factor applied to the
30 nonce, and that atomically binds an
31 unblinded certificate and a blinded
32 unvalidated certificate to be validated;
33 vi. determine if the second transaction request
34 message has the same nonce, session key,
35 and blinding factor applied to the nonce as
36 the first transaction request message
37 stored in the recovery database;
38 vii. if the second transaction request message
39 has the same nonce, session key, and

Sub
CA03

41 blinding factor applied to the nonce as the
42 first transaction request message, then to
43 retrieve the first transaction response
44 message from the recovery database and send
45 the first transaction response message to
46 the transaction response recipient,
said memory coupled to said processor.

1 20. The apparatus of claim 19, further comprising a port
2 adapted to be coupled to a network, said port coupled to
3 said processor and said memory.

1 21. A medium that stores instructions adapted to be
2 executed by a processor to perform the steps of:

- 3 a. receiving an initialization request message that
4 atomically binds
5 i. authorization data, and
6 ii. a blinded unvalidated certificate to be
7 validated;
8 b. determining if the authorization data is valid;
9 c. if the authorization data is valid, then
10 validating the blinded unvalidated certificate
11 to obtain a blinded validated certificate; and
12 d. sending an initialization response message to a
13 registrant that includes the blinded validated
14 certificate atomically bound to the
15 initialization request message received in step
16 a.

Sub a 2/ 1 22. A medium that stores instructions adapted to be
2 executed by a processor to perform the steps of:

- 3 a. receiving a transaction request message that
4 atomically binds
5 i. an unblinded certificate, and
6 ii. a blinded unvalidated certificate to be
7 validated;
8 b. determining if the unblinded certificate is
9 valid; and
10 c. if the unblinded certificate is valid, then
11 performing a transaction response that includes
12 i. validating the blinded unvalidated
13 certificate to obtain a validated blinded
14 certificate, and
15 ii. sending the validated blinded certificate
16 atomically bound to the transaction request
17 message to a transaction response recipient
18 in a transaction response message.

1 23. A medium that stores instructions adapted to be
2 executed by a processor to perform the steps of:

- 3 a. receiving a transaction request message that
4 atomically binds
5 i. an unblinded certificate,
6 ii. a blinded unvalidated certificate to be
7 validated, and
8 iii. blinded audit data;
9 b. sending an audit request message atomically
10 bound to the transaction request message to an
11 audit recipient;

- Sub
a3
- 12 c. receiving an audit response message atomically
13 bound to the audit transaction message, wherein
14 the audit response message includes audit
15 response data;
16 d. determining if the blinded audit data is valid
17 using the audit response data.

1 24. A system for performing an electronic transaction,
2 comprising:

- 3 a. means for receiving a transaction request
4 message that atomically binds
5 i. an unblinded certificate, and
6 ii. a blinded unvalidated certificate to be
7 validated;
8 b. means for determining if the unblinded
9 certificate is valid; and
10 c. means for validating the blinded unvalidated
11 certificate to obtain a validated blinded
12 certificate; and
13 d. means for sending the validated blinded
14 certificate atomically bound to the transaction
15 request message to a transaction response
16 recipient in a transaction response message.

1 25. The system of claim 24, further comprising means for
2 auditing an electronic transaction.

1 26. The system of claim 24, further comprising means for
2 initializing a series of electronic transactions.

27. The system of claim 24, further comprising means for
recovering from an interruption in an electronic
transaction.

00635778-084100